DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-11110
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esq., Department Counsel
For Applicant: Brian J. Lauri, Esq.

06/28/2012

Decision

NOEL, Nichole L., Administrative Judge:

Applicant contests the Defense Department's intent to deny his eligibility for a security clearance to work in the defense industry. In 2010, Applicant received an unpaid, three-day suspension for violating his employer's information technology and labor-charging policies. Applicant demonstrated rehabilitation and these events do not serve as a potential source for pressure, coercion, exploitation or duress. Clearance is granted.

Statement of the Case

Acting under the relevant Executive Order and DoD Directive,[1] on January 4, 2012 the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) explaining that it was unable to find that it is clearly consistent with the national interest to grant Applicant access to classified information. The SOR, which

[1] This case is adjudicated under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry*, signed by President Eisenhower on February 20, 1960, as amended, as well as DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive). In addition, the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (AG), effective within the Defense Department on September 1, 2006, apply to this case. The AG were published in the Federal Register and codified in 32 C.F.R. § 154, Appendix H (2006). The AG replace the guidelines in Enclosure 2 to the Directive.

detailed the reasons for the action under the use of information technology (IT) systems and personal conduct guidelines, recommended the case be submitted to an administrative judge for a determination to revoke or deny Applicant's access to classified information.

Applicant timely answered the SOR and requested a hearing. The case was assigned to me on February 28, 2012. The hearing took place as scheduled on April 5, 2012. At hearing, Government's Exhibits (GE) 1 and 2 were admitted without objection. Applicant testified and submitted Applicant's Exhibits (AE) A through C, which were also admitted without objection. I received the transcript (Tr.) on April 11, 2012.

Findings of Fact

Applicant is a 30-year-old software engineer. He has held a security clearance since 2005 when he began his employment as a federal contractor. He is unmarried and has no children.[2]

In May 2010, Applicant was confronted by his employer with several allegations that he violated company policy including the misuse of his work computer and improper labor charging. In response to these allegations, Applicant admitted that between March and May 2010, he engaged in the following behavior on his unclassified computer:[3]

Applicant used his network privileges to install three unauthorized software programs onto his work computer: a software download accelerator, a media player, and a tethering program. He used the media player to view and listen to non-work related media on his unclassified computer. The tethering program enabled Applicant to use his mobile phone as a wireless internet connection, which he used to access his employer's network remotely. As a result of accessing the company network in this manner, he was able to bypass the security protocols built into his employer's network. He knew that he did not have permission to download these programs or use an alternative protocol to access his employer's network. He did so believing that these programs would make his job easier.[4]

Applicant also admits to violating his employer's labor-charging policies by working remotely and charging that time to his project without having a teleworking agreement in place. In response to allegations that he spent an excessive amount of time on non-work related media and internet sites, Applicant admitted that he often left these types of websites open or ran media (music, television shows, or movies) on his unclassified computer while he worked on the classified system. He also admitted that he viewed pornography on his work computer once while on a business trip.[5]

[2] Tr. 12-13; GE 1.

[3] Tr. 14-15.

[4] Tr. 16-19.

[5] Tr. 19-33, 50-53.

At the conclusion of an internal investigation by the company's ethics organization in June 2010, Applicant received a three-day, unpaid suspension and a written warning. He was also ordered to complete training on the labor-charging policy and the appropriate use of company assets. In addition, he was warned to expect continued monitoring of his company assets and that a future violation of company policy could result in his termination. Applicant timely completed all required training and executed a telework agreement. Applicant's actions did not compromise his employer's IT system or any classified information.[6]

Since the 2010 incident, Applicant has received two performance reviews. In his 2010 review, Applicant's disciplinary action was briefly mentioned, and he received an above-average rating. In the 2011 performance evaluation, Applicant received a superior rating with no mention of any disciplinary issues during the rating cycle.[7]

During his company's internal investigation and the security clearance adjudication process, Applicant has spoken honestly about his behavior. In his responses to DOHA interrogatories and at hearing he admitted that his actions in 2010 showed lack of judgment.[8]

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, administrative judges apply the guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence.

[6] Tr. 23-24, 43; GE 2.

[7] AE C.

[8] Tr. 47-50, GE 2.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual risk of compromise of classified information.

Section 7 of EO 10865 provides that adverse decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M, Use of Information Technology Systems

The security concern for use of information technology systems is set out in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or inability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The following disqualifying conditions under AG ¶ 40 apply:

> (e) unauthorized use of a government or other information system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

Applicant abused his network privileges by downloading three unauthorized programs. One of these programs resulted in his ability to bypass the security

restrictions on his employer's network. He also admits to using his work computer to access non-work related content including television shows, movies, music and, on one occasion, pornography.

Of the three mitigating conditions available under AG ¶ 41, one is applicable:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

Applicant's misuse of his work computer, which occurred two years ago, seems to have been motivated by convenience, not malice. While Applicant's desire to use new technologies to increase his personal convenience and efficiency remains, he appeared contrite and has learned from his mistakes. His unpaid suspension served as a wake-up call. In the two years since his behavior was discovered, Applicant's work evaluations have been favorable. He is well regarded by his superiors and has since abided by all of his employer's policies regarding the employee use of work assets and IT systems without further incident.

Guideline E, Personal Conduct

The security concern regarding personal conduct is set out in AG ¶ 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following disqualifying conditions under AG ¶ 16 apply:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; and
>
> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or their characteristics indication that the

person may not properly safeguard protected information. This includes, but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the work place;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources.

Applicant admits that he violated his employer's labor-charging practices by working remotely without a telework agreement and spending excessive time on non-work related content on his work computer during duty hours. Furthermore, Applicant's misuse of his work assets and his employer's IT systems is indicative of poor judgment and shows an unwillingness to comply with rules and regulations.

The guideline notes several mitigation conditions under AG ¶ 17. Of these, only one applies:

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

Applicant's violation of the labor-charging polices were minor and easily remedied. Applicant completed the required training and is now in compliance with his employer's teleworking requirements. The infractions were appropriately handled as a personnel issue. Applicant's misuse of IT systems is mitigated under the personal conduct guideline for the same reasons enumerated in the discussion of the use of IT systems guideline, above. These incidents do not cast doubt on Applicant's current security worthiness.

Whole-Person Analysis

I have no reservations or doubts about Applicant's current reliability, trustworthiness, and ability to protect classified information. In reaching this conclusion, I have also considered the whole-person factors at AG ¶ 2. Applicant's conduct was limited to a brief period of time, two months. When confronted, Applicant admitted his behavior, took responsibility for his actions, and immediately stopped the offending conduct. While his actions were wrong, his motivation was benign. Although Applicant, given his technical skills, retains the ability to manipulate his employer's network and

hardware, I find that he has learned not to do so for any reason. At hearing he demonstrated his understanding of the need to comply with his employer's polices and the consequences of failing to do so. His favorable performance evaluations and his total compliance with his employer's polices in the two years since his employer took disciplinary action against him, are strong evidence of rehabilitation. While these events have imparted an important lesson to Applicant, they do not serve as a potential source for pressure, coercion, exploitation or duress. Clearance is granted.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraphs 1.a.:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a.:	For Applicant

Conclusion

In light of all of the circumstances, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Nichole L. Noel
Administrative Judge